SERVICIO DE SOPORTE EN SITIO DE LA PLATAFORMA IBM QRADAR CON QUE CUENTA EL BATALLÓN DE CIBERDEFENSA Y CIBERSEGURIDAD DEL EJÉRCITO NACIONAL
No. JEMPP-CEDE6-BRICC-BACCI-ET-02617/ COMUN-03

CONTENIDO

Elaboró	Revisó	Aprobó
SS. FABIAN OSPITIA BEJARANO Analista Seguridad Interna BACCI	**MY. FABIAN ANDRES BAHENA VASQUEZ** Ejecutivo y Segundo Comandante de Ciberdefensa y Ciberseguridad **MY. JOSE DAVID ALEXANDER MUNEVAR LARA** Oficial Jurídico BRICC	**TC. SILVA GUTIERREZ RAMIRO ESTEBAN** Comandante Batallón de Ciberdefensa y Ciberseguridad

1. OBJETO:

Renovación del servicio de soporte en sitio de los productos de IBM para el Correlacionador de eventos del Batallón de Ciberdefensa y ciberseguridad del Ejército Nacional y todas sus aplicaciones con la que cuenta la Herramienta a la fecha.

2. DEFINICIONES Y APLICACIÓN:

2.1 DEFINICIONES

- **APTS**: Una amenaza persistente avanzada, también conocida por sus siglas en inglés, APT (por Advanced Persistent Threat), es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica. Una APT, generalmente, fija sus objetivos en organizaciones o naciones por motivos de negocios o políticos.

- **CORRELACIONADOR DE EVENTOS**: Un Correlacionador de eventos de seguridad es un sistema Hardware o Software donde se concentran, estandarizan y relacionan logs, de los diferentes dispositivos de una red.

- **BOTNETS**: es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

- **CIBERTERRORISMO**: El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas.

- **HACKTIVISMO**: (un acrónimo de hacker y activismo) se entiende normalmente "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos.

- **MALWARE POLIMÓRFICO**: El malware polimórfico es aquel que es capaz de modificarse a si mismo, normalmente para evitar las protecciones instaladas en el sistema, que suelen buscar coincidencias completas en una base de datos.

- **SIEM**: Security Information and Event Management (SIEM) La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red.

- **SPEAR PHISING**: es una estafa focalizada por correo electrónico cuyo único propósito es obtener acceso no autorizado a datos confidenciales. A diferencia de las estafas por phishing, que pueden lanzar ataques amplios y dispersos, el spear phishing se centra en un grupo u organización específicos. La intención es robar propiedad intelectual, datos financieros, secretos comerciales o militares y otros datos confidenciales.

- **PHISHING**: suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información

2.2. APLICACIÓN

El Ejército Nacional requiere contar con una herramienta que permita fortalecer el Centro de Operaciones de Seguridad (SOC), donde se centraliza la información de múltiples fuentes y además brinde la posibilidad de identificar ataques complejos que afectan múltiples puntos a la vez. Un correlacionador puede tener muchos usos y objetivos, entre los cuales se encuentran:

- Centralizar y almacenar logs por un periodo extendido de tiempo para cumplir con regulaciones de retención de información.
- Normalizar e indexar la información para su fácil búsqueda y análisis.
- Capacidad poderosa de búsqueda para investigación forense.
- Crear reglas de correlación para generar alertas o identificar ataque esperados o conocidos.
- Distintas cualidades de inteligencia de seguridad como análisis heurístico, firmas de ataques, análisis de comportamiento, análisis con inteligencia artificial, suscripciones a servicios de inteligencia, etc.
- Atención a alertas y eventos con corrección automática
- Visualización de información y alertas
- Estadísticas de eventos

3. REQUISITOS:

3.1. REQUISITOS GENERALES

Se requiere la Renovación del servicio de soporte en sitio de los productos de IBM para el Correlacionador de eventos del Batallón de Ciberdefensa y ciberseguridad del Ejército Nacional y todas sus aplicaciones con la que cuenta la herramienta a la fecha, con el fin de proteger la Infraestructura tecnológica del Ejército Nacional, fortaleciendo la compañía de Defensa Cibernética la cual tiene su administración y gestión. La plataforma de IBM consta tanto de hardware como de software el cual debe ser soportado ante cualquier falla por el fabricante, a través de compañías autorizadas; las cuales en su mayoría son empresas en Colombia prestadoras de servicios de seguridad de la información.

3.2 Requisitos Específicos

3.2.1 “SERVICIO DE SOPORTE TECNICO ESPECIALIZADO EN SITIO”	
ITEM	CARACTERISTICA:
3.2.1.1	Consiste en todas aquellas tareas de administración, configuración, solución de fallas y cualquier actividad relacionada al correcto funcionamiento y actividades de aseguramiento de la plataforma, módulos y herramientas con los que cuenta el Correlacionador de eventos del Ejército Nacional y su gestión, garantizando la disponibilidad 100% de la plataforma. Las actividades que se deben realizar en el servicio de soporte en sitio son: 1. Levantamiento de la información. 2. Revisión y afinamiento de los sistemas que involucran la plataforma IBM QRadar SIEM, IBM QRadar, IBM QRadar Vulnerability Manager, realizar la afinación y creación de nuevo playbook el SOAR IBM para automatización de la herramienta de correlación de eventos QRadar y todas las aplicaciones desplegadas sobre la herramienta. 3. Análisis de la información. 4. Validación de las actualizaciones de software. 5. Evaluación proactiva de potenciales problemas. 6. Análisis de ambientes: análisis de ambiente de ejecución de los productos de software IBM cubiertos. 7. Soporte Nivel 1 y Nivel 2 de acuerdo lo requerido 8. Soporte Remoto.

	9. Soporte al proceso de instalación de la arquitectura recomendada 10. Soporte para las actividades de instalación de los productos de software IBM cubiertos 11. Soporte y recomendaciones de mejores prácticas. 12. Soporte para la integración de nuevas fuentes de eventos. 13. Soporte para la creación de ofensas. 14. Soporte para instalación de aplicaciones de Qradar. 15. Manejo de casos de soporte. 16. Integración de Orígenes de fuentes para Qradar. 17. Creación, pruebas y ajustes de casos de uso. 18. Creación, pruebas y ajustes de reglas de correlación. 19. Afinamiento de los todos los módulos de IBM Qradar con que cuenta la fuerza. 20. Transferir conocimiento al personal encargado de la administración de la plataforma IBM. 21. El contratista debe brindar atención ilimitada a casos reportados por el Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional, referentes a cualquier evento relacionado con el funcionamiento, administración e incidentes o eventos de seguridad de las plataformas de seguridad informática integrada al correlacionador de eventos Q-RADAR. 22. El contratista debe realizar un informe detallado al inicio del contrato, durante los primeros cinco días hábiles, en el cual se evidencie el estado actual de la herramienta de correlación de eventos QRadar con sus respectivos módulos y aplicativos (Fortalezas, debilidades, aspectos por mejorar). 23. Verificación actual de la topología general física y lógica de la herramienta con sus respectivos módulos y aplicativos, en caso tal de requerirse deberá actualizarse y registrar cualquier cambio que ocurra durante el contrato. 24. Actualización de la herramienta de correlación de eventos QRadar con sus respectivos módulos y aplicativos a la última versión funcional de acuerdo a la página web de descargas y actualizaciones de IBM QRadar; garantizando el funcionamiento y disponibilidad de la herramienta, con las responsabilidades que este ejercicio requiera como lo serian Backups, afinamiento y puesta en funcionamiento de la nueva versión y/o equipo a implementar. 25. Levantamiento de dispositivos que están enviando logs al QRadar, con el fin de evidenciar:

	• Su estado actual (funcional, ultima llegada de logs, configuración) • La información recibida representa valor a la correlación de eventos • Logs enviados de fuentes desconocidas (formatos sin parcear) Seguido a esto se debe incluir como punto en el plan de trabajo para darle solución puntual a los problemas evidenciados. 26. Revisión, afinamiento y puesta en funcionamiento operacional (sincronía de cada elemento, modulo y/o aplicación que componen la solución) de los sistemas que involucran la plataforma IBM QRadar SIEM así: IBM Collector IBM Console IBM QRadar Vulnerability Manager. IBM SOAR configuración y afinamiento. Se debe garantizar que cada módulo anteriormente descrito y los demás que se instalen en el desarrollo del contrato, se encuentre en correcto funcionamiento para la labor que debe desempeñar atendiendo las mejores prácticas emitidas por IBM QRadar. 27. Realizar un análisis de las aplicaciones con las que actualmente cuenta la herramienta; con el objetivo de recomendar, descargar instalar afinar y poner en funcionamiento nuevas aplicaciones y que estas den valor y soporte a la operación. 28. Se debe realizar una afinación exhaustiva del canal “Offenses”, alimentado, con casos de uso, excepciones (comportamiento, trafico, reglas de correlación, etc.) indicadores de compromiso, listas negras, inteligencia de otras fuentes, mencionado canal será la ventana de consulta y visualización de operadores y analistas del Centro de Operaciones de Seguridad del Ejercito SOC-EJC. 29. Creación de reglas de correlación, reportes, Dashboards, alertas que permitan y mejoren la operación dentro del SOC-EJC. 30. La inclusión, integración, afinamiento y puesta en funcionamiento de nuevas fuentes soportadas por IBM QRadar.

	31. En caso tal de ser requerido, el soporte debe tomarse de forma remota cubriendo el manejo de casos de soporte con Nivel 2 y Nivel 3. 32. Cuando el técnico se encuentre en sitio, debe estar acompañado del administrador de la herramienta o al menos un analista de operación, de la misma forma cada ticket creado con soporte de fábrica debe quedar retroalimentado con el fin de identificar el trabajo realizado; es importante resaltar que la transferencia de conocimientos debe ser continua y explicita cuando se requiera por parte de los analistas de la compañía de defensa cibernética de la unidad. 33. En sitio con personal especializado (en caso de que se requiera).
3.2.1.2	El Contratista deberá garantizar el normal funcionamiento de la plataforma después de algún afinamiento o actualización, de no ser así el contratista deberá cubrir los gastos que se generan para reestablecer la plataforma en un tiempo no mayor a 24 horas.
3.2.1.3	**DISPONIBILIDAD** • Se requiere que el contratista brinde soporte remoto especializado sobre la plataforma en la disponibilidad 7x24. • El contratista deberá brindar soporte técnico especializado de forma remota cuando lo requiera la entidad y cuando se necesite soporte especializado (tener en cuenta sábados, domingos y festivos).

3.3.1 Empaque.

OMITIDO

1.3.2 Rotulado.

OMITIDO

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

4.1.1 Muestreo.

OMITIDO

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado.

OMITIDO

4.2 TOMA DE MUESTRAS Y CRITERIOS DE ACEPTACIÓN O RECHAZO PARA EVALUAR REQUISITOS ESPECÍFICOS.

4.2.1 Muestreo.

OMITIDO

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos

OMITIDO

5. MÉTODOS DE ENSAYO:

OMITIDO

6. APÉNDICE:

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia.
- Código Civil.
- Código General del Proceso.
- Código de Comercio.
- Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

- Ley 80 de 1993 “Por la cual se expide el Estatuto General de Contratación de la Administración Pública” y las demás normas que la modifiquen o aclaren.
- Ley 816 de 2003 “Por medio de la cual se apoya a la industria nacional a través de la contratación pública” y las demás normas que la modifiquen o aclaren.
- Ley 1150 de 2007 “Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos” y las demás normas que la modifiquen o aclaren.
- Ley 1341 de 2009 “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones” y las demás normas que la modifiquen o aclaren.
- Ley 1474 de 2011 “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública” y las demás normas que la modifiquen o aclaren.
- Decreto Ley 19 de 2012 “Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública” y las demás normas que lo modifiquen o aclaren.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones” y las demás normas que la modifiquen o aclaren.
- Decreto 1082 de 2015 “por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional” y las demás normas que lo modifiquen o aclaren.
- Decreto 103 del 20 de enero de 2015 “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones” y las demás normas que lo modifiquen o aclaren.
- Resolución 2710 de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones “Por la cual se establecen lineamientos para la adopción del protocolo IPv6”, modificada por la resolución No. 1126 de 2024 y las demás normas que la modifiquen o aclaren.
- Resolución 4223 de 2022 “Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa nacional, unas funciones de carácter administrativo y se dictan otras” y las demás normas que la modifiquen o aclaren.

- Resolución 4130 de 2022 “MANUAL DE CONTRATACIÓN Y DE CONVENIOS” del Ministerio de Defensa Nacional y las demás normas que la modifiquen o aclaren.
- Resolución 7870 de 2022 del Ministerio de Defensa, Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa y se dictan otras disposiciones.
- Directiva permanente 00201 de 2017 “Lineamiento de ciberseguridad y Ciberdefensa para el Ejercito Nacional” y las demás normas que la modifiquen o aclaren.
- Directiva permanente 00221 de 2017 “Seguridad de la información para el Ejercito Nacional” y las demás normas que la modifiquen o aclaren.
- Procedimiento documentos técnicos normativos P-JEMPP-CEDE4-348

6.2 ANTECEDENTES

El año 2019 se suscribe el contrato de prestación de servicios No. 223 - DIADQ-CADCO-CENAC TELEMATICA 2019 CELEBRADO ENTRE EL MINISTERIO DE DEFENSA NACIONAL– EJÉRCITO NACIONAL- DIADQ- CADCOCENAC TELEMATICA Y LA FIRMA UNBIT LTDA PARA EL “MANTENIMIENTO SOPORTE DE LA PLATAFORMA IBM SECURITY Q-RADAR INCIDENT FORENSIC Y BAL ANCEADOR (GAOCC) CIBERDEFENSA, MANTENIMIENTO SOPORTE PLATAFORMA IBM QRADAR (SIEM), A EJECUTAR EN LA VIGENCIA 2019-2020”.

7. ANEXOS:

OMITIDO

8. CONTROL DE REVISIONES:

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación de la especificación técnica SERVICIO DE SOPORTE EN SITIO DE LA PLATAFORMA IBM QRADAR DE LA UNIDAD DE CIBERDEFENSA DEL EJÉRCITO NACIONAL No. JEMPP-CEDE4-DIETE-ET-02617/ COMUN-0	13/10/2020.
01	Modificación Numeral 1 objeto del contrato, 2.2 aplicación, 3.1 requisitos generales, en los requisitos específicos numerales 1.3,1.4,1.6. Por lo anterior, queda sin validez la versión SERVICIO DE SOPORTE EN SITIO DE LA PLATAFORMA IBM QRADAR DE LA UNIDAD DE	11/10/2022

SERVICIO DE SOPORTE EN SITIO DE LA PLATAFORMA IBM QRADAR CON QUE CUENTA EL BATALLÓN DE CIBERDEFENSA Y CIBERSEGURIDAD DEL EJÉRCITO NACIONAL No. JEMPP-CEDE6-BRICC-BACCI-ET-02617/ COMUN-03

	CIBERDEFENSA DEL EJÉRCITO NACIONAL No. JEMPP-CEDE4-DIETE-ET-02617/ COMUN-0 y a partir del momento rige la presente versión.	
02	Modificación, a los, item 1.1, 1.2 “El contratista deberá brindar servicio de soporte técnico especializado en sitio durante la ejecución del contrato en horario 3x8. 1.2 Se requiere que el Contratista proporcione un ingeniero en sitio en horario de 8 am a 5 pm (03) tres días a la semana. Modificación Numeral 3 objeto del contrato, 3.1 requisitos generales, en los requisitos específicos, item 1.6, agregando 01 curso como soporte por parte del ingeniero en sitio. IBM SECURITY SOAR (Resilient)	03/05//2023
03	Se realizaron las siguientes modificaciones a la especificación técnica SERVICIO DE SOPORTE EN SITIO DE LA PLATAFORMA IBM QRADAR CON QUE CUENTA EL BATALLÓN DE CIBERDEFENSA Y CIBERSEGURIDAD DEL EJÉRCITO NACIONAL ASI: • Se actualiza la especificación técnica en atención al oficio radicado Nª 2024574004746513 de fecha 27 de febrero del año 2024, en cumplimiento a la circular 2023218004540933 del 09 de marzo y el boletín 030 del 17 de febrero 2023 emitido por JEMPP, acogiéndose al numeral 02. Del boletín 030 del 17 de febrero de 2023: por mejora del documento al ser revisado. • Se modifica línea de mando de la especificación técnica de la siguiente manera JEMPP-CEDE6-BACCI-ET-02617 • Eliminación: se realiza la eliminación de los siguientes Ítems en razón a que hacen parte de las especificaciones técnicas adicionales de obligatorio cumplimiento así: • Se realizó la eliminación del Item 1, Confidencialidad de la información en razón a que hace parte de las especificaciones técnicas adicionales de obligatorio cumplimiento. • Se realizó la eliminación Item 1.1teniendo en cuenta que se encuentra duplicado con el Ítem 1.2 • Se realizó la eliminación Ítem 1.6 perfil del Ingeniero en razón a que hace parte de las especificaciones técnicas adicionales de obligatorio cumplimiento. • Se realizó la eliminación Ítem 1.7 desempeño profesional en razón a que hace parte de las especificaciones técnicas adicionales de obligatorio cumplimiento. • Se realizó la eliminación Ítem 1.8 Propiedad Intelectual en razón a que hace parte de las especificaciones técnicas adicionales de obligatorio cumplimiento. • Se realizó la eliminación ítem 1.9 Documentación en razón a que hace parte de las especificaciones técnicas adicionales de obligatorio cumplimiento. • Se realizó la eliminación ítem 2.0 certificaciones partner en razón a que hace parte de las especificaciones técnicas adicionales de obligatorio cumplimiento.	13/03/2024

	• Se realizó la Modificación de la numeración a partir de Item 3.2 Requisitos Específicos • Se realizó la Modificación del Ítem 1.2, teniendo en cuenta que el presente Ítem hace relación a que el contratista proporcione el ingeniero en un horario de 5x8 • Se realizó la Modificación del Ítem 1.4 en razón a que el SOAR ya se encuentra desplegado y se requiere es afinar y la creación de nuevo playbook • Se realizó la Modificación del Item 2.2 Aplicación donde se realiza la modificación al texto de explicación. • Se modifica el item 6.1 1 Normas que deben consultarse, se actualiza la normatividad, de acuerdo a lo mencionado por el Asesor Jurídico de la Brigada de Interoperabilidad de Comunicaciones, Computación y Ciberdefensa. • El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza la pluralidad de oferentes. • El Batallón de Ciberdefensa y Ciberseguridad BACCI, en la presente especificación técnica garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional. • El Batallón de Ciberdefensa y Ciberseguridad BACCI, técnica garantiza que la presente especificación fue elaborada de manera profesional, con la mayor transparencia, siempre buscando dejar en alto el nombre del Ejército Nacional. • Por lo anterior, queda sin validez la especificación técnica versión 2 y a partir del momento rige la presente versión.	